UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,114	09/10/2004	Andrea Soppera	36-1838	4734

23117 7590 04/24/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,114	SOPPERA, ANDREA	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 September 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/8/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for priority. ***Information Disclosure Statement***

3. The information disclosure statement (IDS) submitted on 08 June 2005 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

Drawings

4. Figures 1, 2, and 3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated and their related description on pages 3-5 of the Specification are related to the state of the art at the time the invention was filed. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading: .

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

The disclosure is objected to because of the following informalities:

The Applicant has failed to provide any of the Section Headings disclosed above.

6. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 38-45 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See

MPEP § 2172.01. Claims 38-45 are directed toward a key distribution system, but fail to recite any structural elements that would comprise the system. In fact, the claim limitations of claim 38 amount to nothing more than nonfunctional descriptive data.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1, 2, 5-16, 21, 22, and 25-43 are rejected under 35 U.S.C. 102(b) as being anticipated by **ELK, a New Protocol for Efficient Large-Group Key Distribution**, to Adrian Perrig et al., hereinafter Perrig.

11. As per claims 1 and 21, Perrig teaches a method and system (page 10, section 7.2) of managing keys in a key distribution system for a communications group, the key distribution system maintaining a tree of nodes including at least one leaf node that has a parent node, each node of the group being associated with a first key, the method comprising:

the system updating the first keys of a first branch of nodes in the tree by allocating new first keys to each of the nodes in the branch (page 7, Figure 2, Section 6.2.1);

the system determining an offset for generating the updated first key of each node in the branch from the previous node in the branch (page 7, Section 6.2.1, page 8, Sections 6.2.2, 6.2.3, page 10, Sections 7.2, 7.3, i.e. *a* is the number of updated keys, or keys for time intervals); and

broadcasting each of said offsets so that, given the updated first key associated with the first node of said branch, each updated first key of said branch of nodes can be calculated (page

8, Sections 6.2.2, 6.2.3, page 10, Sections 7.2, 7.3, i.e. hint messages where *a* is the number of updated keys).

12. Regarding claims 2 and 43, Perrig teaches wherein the first key of each parent node in said tree of nodes is generated from the first key of each of its child nodes by two one-way functions and a mixing function, the mixing function including the offset as a parameter (page 5, Section 6.1.1, page 6, Procedure 1).

13. Regarding claims 5, 26, and 39, Perrig teaches wherein the communication group comprises at least one member that is associated with a leaf node of the tree of nodes (page 3, Figure 1, Section 4.2).

14. With regards to claims 6 and 27, Perrig teaches wherein information transferred to, from or between members of the communication group is encrypted using an application data encryption key (page 1, Section 1), the encryption key comprising a join field and a leave field, wherein each member of the group knows the join field of the encryption key (page 7, Section 6.2.1, Protocol 1), and wherein the leave field of the encryption key is derived from the first key of a root node of the tree (page 8, Sections 6.2.2, 6.2.3).

15. Concerning claims 7, 28, and 40, Perrig teaches wherein the join field of the encryption key is updated each time a member joins the group (page 7, Section 6.2.1, Protocol 1).

16. Concerning claims 8 and 29, Perrig teaches wherein the new member joins the group using the following method:

the new user requests access to the group (page 3, Section 4.2, Figure 1);

the new user is granted access to the group (page 3, Section 4.2, Figure 1);

the new member is assigned a node at a new leaf node of the communication group (page 4, Section 4.2, page 7, Figure 2, Section 6.2.1, protocol 1);

the new member is sent all the information required to generate the first key of each node on a branch of nodes from the new leaf node to the root node (page 4, Section 4.2, page 7, Figure 2, Section 6.2.1, protocol 1); and

the join field of the application data key is updated (page 7, Section 6.2.1, Protocol 1).

17. Concerning claims 9 and 30, Perrig teaches the generation of a new node as the parent of both the new leaf node and a pre-existing node (page 7, Section 6.2.1, Figure 2).

18. Concerning claims 10, 31, and 41, Perrig teaches wherein the updated join field is generated from the previous join field using a one-way function (page 2, Section 3, page 7, Section 6.2.1, Protocol 1, i.e. pseudo-random functions).

19. Concerning claims 11, 32, and 42, Perrig teaches wherein a key update request is generated each time a member leaves the group, wherein the first keys of each node of the branch of nodes including both the node associated with the member that is leaving the group and the root node are the keys that are updated (page 8, Sections 6.2.2, 6.2.3, page 9, example 1).

20. Concerning claims 12 and 33, Perrig discloses wherein a member leaves the group using the following method:

an instruction to remove a member from the group is generated (page 1, Section 1, pages 3-4, Section 4.2);

the parent node of the node associated with the leaving member is deleted (page 8, Figure 3, Sections 6.2.2, 6.2.3, page 9, Example 1);

the sibling node of the node associated with the leaving member is promoted to the position occupied by the deleted node (page 8, Figure 3, Sections 6.2.2, 6.2.3, page 9, Example 1);

the first key of each node on the branch of nodes from the promoted node to the root node is updated (page 8, Figure 3, Sections 6.2.2, 6.2.3, page 9, Example 1);

offset messages for generating the new first keys are broadcast to the group (page 8, Figure 3, Sections 6.2.2, 6.2.3, page 9, Example 1);

remaining members of the communications group calculate the updated first key nodes of the tree (page 8, Figure 3, Sections 6.2.2, 6.2.3, page 9, Example 1).

21. Concerning claims 13 and 34, Perrig teaches wherein the instruction to remove a member from the group is generated by the member that is leaving the group (page 8, Figure 3, Sections 6.2.2, 6.2.3, page 9, Example 1).

22. Concerning claims 14 and 35, Perrig does not explicitly state that the instruction to remove a member from the group is generated by a key distribution server. It is a well-known and common practice in the art of key distribution via hierarchical trees for the key distribution server to evict a leaf node and Official Notice is taken of such.

23. Regarding claims 15 and 36, Perrig teaches wherein the nodes are arranged in a hierarchical tree (page 3, Figure 1, Section 4.2, page 7, Figure 2, page 8, Figure 3).

24. With regards to claims 16 and 37, Perrig teaches wherein the nodes are arranged in a binary tree (page 3, Figure 1, Section 4.2, page 7, Figure 2, page 8, Figure 3).

25. As per claim 22, Perrig teaches a key distribution system for a communications group, the key distribution system maintaining a tree of nodes including at least one leaf node that has a parent node, each node being associated with a first key, wherein:

the first key of each parent node in the tree is derived from the first key of each of its child node by two one-way functions and a mixing function, the mixing function including an offset value as a parameter (page 5, Section 6.1.1, page 6, Procedure 1 page 8, Sections 6.2.2, 6.2.3, page 10, Sections 7.2, 7.3).

26. Regarding claim 25, Perrig teaches wherein the first keys of a first chain of nodes along a branch of the tree are updated by allocating new first keys to each of those nodes in response to a request to update the first keys of that chain of nodes (page 7, Figure 2, Section 6.2.1);

an offset for generating the updated first key of each member of the chain from the previous member of the chain is determined (page 7, Section 6.2.1, page 8, Sections 6.2.2, 6.2.3, page 10, Sections 7.2, 7.3, i.e. *a* is the number of updated keys, or keys for time intervals); and

each of said offsets is broadcast so that, given the updated first key associated with the first node of said chain of nodes, each updated first key on said chain of nodes can be calculated (page 8, Sections 6.2.2, 6.2.3, page 10, Sections 7.2, 7.3, i.e. hint messages where *a* is the number of updated keys).

27. As per claim 38, Perrig teaches key distribution system for a communications group, the key distribution system comprising an encryption key and maintaining a tree of nodes including a root node that has at least one child node, and at least one leaf node that has a parent node, the communication group comprising at least one member, wherein the encryption key comprises a join field and a leave field, and wherein:

each member of the group knows the join field of the encryption key (page 7, Section 6.2.1, Protocol 1);

each node of the key distribution system is associated with a leave key (page 8, Sections 6.2.2, 6.2.3);

the leave field of the encryption key is derived from the leave key of the root node (page 8, Sections 6.2.2, 6.2.3).

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

29. Claims 3, 4, 23, 24, 44, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perrig in view of U.S. Patent No. 6,240,188 to Dondeti et al., hereinafter Dondeti.

30. With regards to claims 3, 23, and 44, Perrig does not teach wherein the mixing function in an XOR function.

31. Dondeti teaches wherein the mixing function in an XOR function (column 8, lines 24-43).

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made using an XOR mixing function, since Dondeti states at column 8, lines 41-42 that using an XOR mixing function is more efficient with respect to storage and requires less processing time to computer internal node keys.

33. With regards to claims 4, 24, and 45, Perrig teaches wherein each parent key is generated using the formula f(f (child key) OFFSET), wherein OFFSET is the offset and f represents a one-way function and wherein child key is the first key of a child node of said parent node (page 5, Section 6.1.1, page 6, Procedure 1).

34. Perrig does not teach the XOR function.

35. Dondeti teaches an XOR function mixing function (column 8, lines 24-43).

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made using an XOR mixing function, since Dondeti states at column 8, lines 41-42 that

using an XOR mixing function is more efficient with respect to storage and requires less processing time to computer internal node keys.

37. Claims 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perrig in view of U.S. Patent No. 5,146,497 to Bright, hereinafter Bright.

38. Regarding claim 17, Perrig does not teach retransmitting messages enabling, users to update keys in case the users have not received those messages.

39. Bright teaches resending the rekeying information (column 2, lines 12-23, claims 1 and 8).

40. It would have been obvious to one of ordinary skill in the art at the time the invention was made to retransmit messages enabling users to update keys in case the users have not received those messages, since Bright stats at column 4, lines 8-14 that would allow users that were not powered up at the rekeying time to update the key information.

41. With regards to claim 18, Perrig teaches wherein the retransmitted messages are attached to application data packets (page 9, Section 6.4, i.e. hints carried in data packets).

42. With regards to claim 19, Perrig teaches wherein the retransmitted messages contain a sequence number indicative of the position in the sequence of key updates (page 7, Section 6.2.1, page 8, Sections 6.2.2, 6.2.3, page 10, Sections 7.2, 7.3, i.e. a is the number of updated keys, or keys for time intervals).

43. Concerning claim 20, Perrig teaches wherein the sequence number is cyclic (page 7, Section 6.2.1, page 8, Sections 6.2.2, 6.2.3, page 10, Sections 7.2, 7.3, i.e. *a* is the number of updated keys, or keys for time intervals).

Conclusion

44. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

45. The following patents are cited to further show the state of the art with respect to key distribution systems, such as:

United States Patent No. 7,131,010 to Okaue et al., which is cited to show a key distribution system.

United States Patent No. 7,103,185 to Srivastava et al., which is cited to show distributing and updating private keys of a multicast group.

United States Patent Application Publication No. 2003/0044017 to Briscoe, which is cited to show key management and distribution.

United States Patent No. 6,240,188 to Dondeti et al., which is cited to show a distributed group key management scheme.

46. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

47. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

48. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf